ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.41

Н.С. МОГИЛЕВСКАЯ, К.С. СУХОСТАВСКАЯ

ОБ ЭКСПЕРИМЕНТАЛЬНОМ ИССЛЕДОВАНИИ ХАРАКТЕРИСТИК МОДИФИЦИРОВАННЫХ ПОМЕХОУСТОЙЧИВЫХ БЛОЧНЫХ ДВОИЧНЫХ КОДОВ

Рассмотрены различные методы модификации помехоустойчивых двоичных блочных кодов. Построено программное средство, реализующее рассмотренные методы и определяющее параметры модифицированных кодов. Проведены вычислительные эксперименты по исследованию характеристик модифицированных помехоустойчивых кодов.
***Ключевые слова**: помехоустойчивое кодирование, методы модификации кодов, матрица.*

Введение. Одним из способов обеспечения защиты от ошибок в системах связи является применение помехоустойчивых кодов. На сегодняшний день известно большое количество кодов с хорошими корректирующими способностями [1-3]. Однако существующие коды не всегда подходят для конкретных практических приложений по таким параметрам, как длина кода, размерность или минимальное кодовое расстояние. Новый код с требуемыми характеристиками можно получить на основе известного кода с помощью одного из методов модификации кодов. При этом длину и размерность нового кода можно определить заранее, а априорное вычисление таких параметров, как минимальное кодовое расстояние и весовой спектр модифицированного кода, либо затруднительно, либо невозможно [2, 3].

Постановка задачи. На основании вычислительных экспериментов исследовать изменение характеристик модифицированных помехоустойчивых кодов по отношению к исходным кодам. Для проведения экспериментов создать программное средство, позволяющее модифицировать заданные коды и находить такие характеристики кода, как минимальное кодовое расстояние, число исправляемых и обнаруживаемых ошибок, скорость и весовой спектр.

Основные методы модификации. Опишем кратко суть таких методов модификации, как укорочение, удлинение, расширение, перфорация (выкалывание), пополнение и выбрасывание [2, 3]. Обозначим через **C** линейный блочный (n, k, d)-код над полем **GF(q)** с порождающей матрицей **G** и проверочной матрицей **H**, где n – длина кода, k – размерность кода, d – минимальное кодовое расстояние.

Укорочение кода **C** производится с помощью уменьшения числа информационных символов кода. Пусть порождающая матрица **G** кода **C** задана в систематическом виде, тогда порождающая матрица $\mathbf{G}_s$ укороченного (n-s, k-s, d_s)-кода может быть получена удалением s (0<s<k)-столбцов единичной подматрицы I_k и s строк, соответствующих ненулевым элемен-

там удаляемых столбцов. Связь минимальных расстояний исходного и модифицированного кода: $d_s \geq d$.

Расширение кода **C** означает добавление ε проверочных символов. Расширенный $(n+\varepsilon,\ k,\ d_{ext})$-код $\mathbf{C}_{ext}$ имеет минимальное расстояние $d_{ext} \geq d$. Расширенная проверочная матрица $\mathbf{H}_{ext}$ размером $(n\text{-}k+\varepsilon)\times(n+\varepsilon)$ получается из проверочной матрицы исходного кода **C** добавлением ε столбцов и ε строк. Наиболее известный и часто используемый способ расширения состоит в добавлении общей проверки на четность:

$$H_{ext} = \begin{matrix} 1 & 1 \ \dots \ 1 \\ 0 & \\ 0 & H \\ 0 & \end{matrix}.$$

Известно, что в общем случае коды, расширенные проверкой на четность, обладают минимальным расстоянием d_{ext} на единицу превышающего минимального расстояния исходного кода d_{min}, если значение d_{min} – нечетное, и d_{ext} совпадает с d_{min} в случае четного значения d_{min}.

Перфорация линейных блочных кодов состоит в удалении проверочных символов, что приводит к блочному $(n\text{-}p,\ k,\ d_p)$-коду $\mathbf{C_p}$ с минимальным расстоянием $d_p<d$. Для проведения перфорации используется матрица **H** в систематическом виде. Проверочная матрица $\mathbf{H_p}$ перфорированного кода $\mathbf{C_p}$ получается удалением p-столбцов единичной подматрицы $I_{n\text{-}k}$ матрицы **H** и p-строк матрицы **H** исходного кода, соответствующих ненулевым элементам удаляемых столбцов.

Пополнение кода означает добавление линейно независимых строк к порождающей матрице кода, а выбрасывание состоит в удалении строк из порождающей матрицы.

Программное средство. В данной работе построено программное средство, которое позволяет, во-первых, модифицировать блочные двоичные коды произвольной размерности такими методами, как укорочение, расширение, выкалывание, дополнение и выбрасывание, во-вторых, определяет важные характеристики блочных двоичных кодов.

На вход программы подаются длина и размерность исходного кода и одна из его матриц: проверочная H или порождающая G. Если введенная матрица находится в несистематическом виде, то программа автоматически преобразует ее в систематический вид с использованием метода Гаусса. Если не удается достичь нужного результата, метод Гаусса дополняется операцией перестановки столбцов. Отметим, что если производится преобразование введенной матрицы и приведение ее к систематическому виду (с применением операции перестановки столбцов или без ее использования), то фактически в дальнейших исследованиях будет исследован не указанный пользователем код **C**, а эквивалентный ему код **C′**. Указанная особенность не изменяет достоверность исследования, так как известно, что все характеристики эквивалентных кодов совпадают [1-3].

По введенной матрице автоматически вычисляется связанная с ней матрица: по матрице **H** вычисляется матрица **G**, а по **G** вычисляется матрица **H.** По матрицам **G** и **H** вычисляются минимальное кодовое расстояние, весовой спектр кода, число гарантированно обнаруживаемых и исправляемых ошибок, а также значения границ Хемминга и Плоткина. Отметим, что

вычисление весового спектра это трудоемкая задача и с ростом длины кода значительно увеличивается время его вычисления. Далее по матрицам **G** и **H** производится проверка, является ли код самодуальным, и создается текстовый отчет, содержащий характеристики исходного кода. Затем пользователем выбирается из списка один из методов модификации кодов. Программное средство автоматически производит модификацию исходного кода, вычисляет характеристики полученного кода и добавляет эти сведения в генерированный ранее отчет.

Таким образом, на выходе работы программы содержится тестовый отчет, содержащий порождающую и проверочную матрицы исходного кода, название и параметры используемого метода модификации, порождающую и проверочную матрицы модифицированного кода, а также длину, размерность, минимальное кодовое расстояние, число исправляемых и обнаруживаемых ошибок и весовой спектр исходного и модифицированного кодов.

Рассмотрим особенности программной реализации методов модификации кодов. При укорочении, перфорации и выбрасывании пользователем указываются номера удаляемых элементов матрицы. Модификация расширением производится только с помощью добавления общей проверки на четность. Модификация дополнением происходит в два этапа: сначала генерируется случайный вектор (линейно независимый по отношению к векторам-строкам матрицы G), затем этот вектор добавляется в качестве нижней строчки к матрице G.

Проведение экспериментов. С помощью разработанного программного средства были проведены эксперименты, цель которых состояла в исследовании возможностей методов модификации кодов. В данной работе приведены результаты модификации кодов Рида-Маллера (РМ-коды) 1-го и 2-го порядков, Хемминга и Голея, а также (17, 10, 3)-кода, чья порождающая матрица была задана случайным образом [1-3].

Результаты экспериментов. В табл.1-5 приведены параметры исходных и модифицированных кодов. Структура таблиц следующая: параметры исходного кода расположены в верхней левой ячейке таблицы и выделены жирным шрифтом, во всех остальных ячейках расположены параметры новых кодов, полученных из исходного применением к нему одного из методов модификации кодов. Название использованного метода модификации указано в верхней строке соответствующей ячейки. В таблицах использовались следующие обозначения: v=k/n – скорость кода; d – минимальное кодовое расстояние; t(и) и t(о) – число гарантированно исправляемых и обнаруживаемых ошибок, соответственно. Весовой спектр кода представлен в виде вектора (a_0, a_1, …, a_i, …, a_n), где a_i – количество кодовых слов веса i.

Результаты экспериментов показывают, что укороченный код исправляет большее число комбинаций ошибок, чем исходный, что подтверждается границей Хемминга. Недостатком укорочения является уменьшение скорости кода. Одним из преимуществ рассматриваемого метода модификации является возможность использовать для укороченного кода те же алгоритмы кодирования и декодирования, что и для исходного кода, добавляя в недостающие позиции слов нули.

Расширение РМ-кодов 1-го и 2-го порядка путем добавления общей проверки на четность не увеличивает корректирующую способность кода.

Этот факт объясняется особым строением проверочной матрицы исходного кода. Расширение (23, 12, 7)-кода Голея дает известный (24, 12, 8)-код Голея, который позволяет обнаруживать большее число ошибок.

Выкалывание кодов в общем случае ухудшает их корректирующие характеристики, в то время как скорость выколотых кодов возрастает по сравнению с исходными. При выкалывании одного столбца РМ-кодов или произвольных двоичных кодов с четным d_{min} полученный модифицированный код позволяет исправлять такое же количество ошибок, а обнаруживать на одну меньше. При выкалывании одного столбца кодов Голея, Хемминга и произвольных двоичных кодов с нечетным d_{min} полученный код может обнаруживать и исправлять ошибки на одну меньше, чем исходный.

В кодах, модифицированных выбрасыванием, увеличивается число проверочных символов и уменьшается число информационных символов, следовательно, модифицированные коды могут исправлять большее число ошибок, чем исходные. При этом скорость модифицированных выбрасыванием кодов значительно уменьшается по сравнению со скоростью исходных кодов.

При модификации пополнением скорость и число информационных символов увеличивается. Отметим также, что результаты рассматриваемого метода модификации зависят от выбранного для пополнения вектора. Пополнение кодов Хемминга и РМ-кодов линейно независимым вектором уменьшает их минимальное кодовое расстояние и, следовательно, ухудшает корректирующие способности кода. Результаты экспериментов показали следующую особенность: спектры модифицированных пополнением РМ-кодов совпадают в случае, если их минимальное расстояние одинаковое, вне зависимости от векторов, использованных для пополнения. К сожалению, в настоящее время авторы не могут привести теоретическое обоснование данному факту. В проведенных экспериментах были найдены случайные коды, которые после модификации пополнением сохраняли такое же минимальное расстояние, как и исходные коды (см.табл.5).

Известно, что для циклических кодов характерен симметричный вид весового спектра. Эта особенность циклических кодов всегда нарушается при модификации их укорочением и практически всегда при модификации их выбрасыванием (за исключением кодов малой длины).

Таблица 1

Результаты модификации (7, 4, 3)-кода Хемминга

Код Хемминга **k=4; n=7; v=0,5714; d=3; t(и)=1; t(о)=2** **Спектр (1, 0, 0, 7, 7, 0, 0, 1)**	Перфорация k=4; n=6; v=0,6667; d=2; t(и)=0; t(о)=1 Спектр (1, 0, 3, 8, 3, 0, 1)
Укорочение k=3; n=6; v=0,5; d=3; t(и)=1; t(о)=2 Спектр (1, 0, 0, 4, 3, 0, 0)	Пополнение Добавлен вектор (0000110) k=5; n=7; v=0,7143; d=1; t(и)=0; t(о)=0 Спектр (1, 1, 3, 11, 11, 3, 1, 1)
Расширение k=4; n=8; v=0,5; d=4; t(и)=1; t(о)=3 Спектр (1, 0, 0, 0, 14, 0, 0, 0, 1)	Выбрасывание k=3; n=7; v=0,4286; d=3; t(и)=1; t(о)=2 Спектр (1, 0, 0, 4, 3, 0, 0, 0)

Таблица 2

Результаты модификации РМ-кода первого порядка

РМ-код 1-го порядка **k=5; n=16; v=0,3125; d=8; t(и)=3; t(о)=7** **Спектр (1, 0, 0, 0, 0, 0, 0, 0, 30, 0, 0, 0, 0, 0, 0, 0, 1)**	Пополнение Добавлен вектор (0111101111000111) k=6; n=16; v=0,375; d=5; t(и)=2; t(о)=4 Спектр (1, 0, 0, 0, 0, 6, 0, 10, 30, 10, 0, 6, 0, 0, 0, 0, 1)
Укорочение k=4; n=15; v=0,2667; d=8; t(и)=3; t(о)=7 Спектр (1, 0, 0, 0, 0, 0, 0, 0, 15, 0, 0, 0, 0, 0, 0, 0)	Пополнение Добавлен вектор (1111010001010011) k=6; n=16; v=0,375; d=5; t(и)=2; t(о)=4 Спектр (1, 0, 0, 0, 0, 6, 0, 10, 30, 10, 0, 6, 0, 0, 0, 0, 1)
Расширение k=5; n=17; v=0,2941; d=8; t(и)=3; t(о)=7 Спектр (1, 0, 0, 0, 0, 0, 0, 0, 30, 0, 0, 0, 0, 0, 0, 0, 1, 0)	Пополнение Добавлен вектор (0111110000100100) k= 6; n = 16 d = 3; t(и) = 1; t(о) = 2 v = 0,375 Спектр (1, 0, 0, 1, 0, 3, 0, 12, 30, 12, 0, 3, 0, 1, 0, 0, 1)
Перфорация k=5; n=15; v=0,3333; d=7; t(и)=3; t(о)=6 Спектр (1, 0, 0, 0, 0, 0, 0, 15, 15, 0, 0, 0, 0, 0, 0, 1)	Выбрасывание k=4; n=16; v=0,25; d=8; t(и)=3; t(о)=7 Спектр (1, 0, 0, 0, 0, 0, 0, 0, 14, 0, 0, 0, 0, 0, 0, 0, 1)

Таблица 3

Результаты модификации РМ-кода второго порядка

РМ-код 2-го порядка **k=11; n=16; v=0,6875; d=4; t(и)=1; t(о)=3** **Спектр (1, 0, 0, 0, 140, 0, 448, 0, 870, 0, 448, 0, 140, 0, 0, 0, 1)**	Пополнение Добавлен вектор (0001101111001100) k=12; n=16; v=0,75; d=2; t(и)=0; t(о)=1 Спектр (1, 0, 8, 0, 252, 0, 952, 0, 1670, 0, 952, 0, 252, 0, 8, 0, 1)
Укорочение k=10; n=15; v=0,6667; d=4; t(и)=1; t(о)=3 Спектр (1, 0, 0, 0, 105, 0, 280, 0, 435, 0, 168, 0, 35, 0, 0, 0)	Пополнение Добавлен вектор (1010100110001011) k=12; n=16; d=2; t(и)=0; t(о)=1; v=0,75 Спектр (1, 0, 8, 0, 252, 0, 952, 0, 1670, 0, 952, 0, 252, 0, 8, 0, 1)
Расширение k=11; n=17; v=0,6471; d=4; t(и)=1; t(о)=3 Спектр (1, 0, 0, 0, 140, 0, 448, 0, 870, 0, 448, 0, 140, 0, 0, 0, 1, 0)	Пополнение Добавлен вектор (1010011100101110) k=12; n=16; d=1; t(и)=0; t(о)=0; v=0,75 Спектр (1, 1, 0, 35, 140, 273, 448, 715, 870, 715, 448, 273, 140, 35, 0, 1, 1)
Перфорация k=11; n=15; v=0,7333; d=3; t(и)=1; t(о)=2 Спектр (1, 0, 0, 35, 105, 168, 280, 435, 435, 280, 168, 105, 35, 0, 0, 1)	Выбрасывание k=10; n=16; v=0,625; d=4; t(и)=1; t(о)=3 Спектр (1, 0, 0, 0, 105, 0, 280, 0, 435, 0, 168, 0, 35, 0, 0, 0, 0)

Таблица 4

Результаты модификации (23, 12, 7)-кода Голея

<table>
<tr><td>Код Голея
k=12; n=23; d=7; t(и)=3; t(о)=6; v=0,5217
Спектр (1, 0, 0, 0, 0, 0, 0, 253, 506, 0, 0, 1288, 1288, 0, 0, 506, 253, 0, 0, 0, 0, 0, 0, 1)</td><td>Перфорация
k=12; n=22; v=0,5455; d=6; t(и)=2; t(о)=5
Спектр (1, 0, 0,0, 0, 0, 77, 352, 330, 0, 616, 1344, 616, 0, 330, 352, 77, 0,0, 0,0, 0, 1)</td></tr>
<tr><td>Укорочение
k=11; n=22; v=0,5; d=7; t(и)=3; t(о)=6
Спектр (1, 0, 0, 0, 0, 0, 0, 176, 330, 0, 0, 672, 616, 0, 0, 176, 77, 0, 0, 0, 0, 0, 0)</td><td>Пополнение
Добавлен вектор (00111011101010010010111)
k=13; n=23; v=0,5652; d=3; t(и)=1; t(о)=2
Спектр (1, 0, 0, 1, 5, 16, 48, 373, 746, 400, 560, 1946, 1946, 560, 400, 746, 373, 48, 16, 5, 1, 0, 0, 1)</td></tr>
<tr><td>Расширение
k=12; n=24; v=0,5; d=8; t(и)=3; t(о)=7
Спектр (1, 0, 0, 0, 0, 0, 0, 0, 759, 0, 0, 0, 2576, 0, 0, 0, 759, 0, 0, 0, 0, 0, 0, 0, 1)</td><td>Выбрасывание
k=10; n=16; v=0,625; d=4; t(и)=1; t(о)=3
Спектр (1, 0, 0, 0, 105, 0, 280, 0, 435, 0, 168, 0, 35, 0, 0, 0, 0)</td></tr>
</table>

Таблица 5

Результаты модификации (17, 10, 3)-кода

<table>
<tr><td rowspan="3">Случайный (17, 10, 3) - код
k=10; n=17; v=0,5882; d=3; t(и)=1; t(о)=2
Спектр (1, 0, 0, 6, 22, 50, 89, 142, 189, 204, 162, 90, 44, 18, 5, 2, 0, 0)
$G =$
10000000000110111
01000000001110110
00100000000111011
00010000001011011
00001000001100000
00000100000001101
00000010001101011
00000001001001101
00000000100111010
00000000011111111</td><td>Укорочение
k=9; n=16; v=0,5625; d=3; t(и)=1; t(о)=2
Спектр (1, 0, 0, 5, 14, 33, 61, 90, 101, 90, 66, 33, 12, 5, 1, 0, 0)</td></tr>
<tr><td>Расширение
k=10; n=18; v=0,5556; d=4; t(и)=1; t(о)=3
Спектр (1, 0, 0, 0, 28, 0, 139, 0, 331, 0, 366, 0, 134, 0, 23, 0, 2, 0, 0)</td></tr>
<tr><td>Перфорация
k=10; n=16; v=0,625; d=1; t(и)=0; t(о)=0
Спектр (1, 1, 1, 9, 31, 72, 119, 162, 199, 193, 135, 69, 25, 6, 1, 0, 0)</td></tr>
<tr><td>Выбрасывание
k=9; n=17; v=0,5294; d=3; t(и)=1; t(о)=2
Спектр (1, 0, 0, 5, 17, 33, 56, 90, 99, 90, 72, 33, 11, 5, 0, 0, 0, 0)</td><td>Пополнение
Добавлен вектор (00010100001001010)
k=11; n=17; v=0,6471; d=3; t(и)=1; t(о)=2
Спектр (1, 0, 0, 13, 38, 95, 195, 294, 373, 398, 318, 185, 84, 35, 15, 4, 0, 0)</td></tr>
</table>

Выводы. Построенное программное средство позволяет модифицировать помехоустойчивые блочные двоичные коды и исследовать характеристики полученных кодов. Его применение позволит разработчикам систем связи сократить время конструирования кодов с наиболее подходящими к конкретной системе связи характеристиками.

Библиографический список

1. Блейхут Р.Э. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1989. – 576 с.
2. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2005. – 320 с.
3. Мак-Вильямс Ф., Слоэн Н. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 583 с.

Материал поступил в редакцию 19.06.07.

N.S.MOGILEVSKAYA, K.S.SUHOSTAVSKAYA

RESEARCH OF CHARACTERISTICS OF THE MODIFIED NOISEPROOF CODES ON THE BASIS OF COMPUTING EXPERIMENTS

In the paper various methods of updating of noiseproof codes are presented, computing experiments on research of characteristics of the modified noiseproof block binary codes are spent.

МОГИЛЕВСКАЯ Надежда Сергеевна, доцент кафедры «Программное обеспечение вычислительной техники и автоматизированных систем» ДГТУ, кандидат технических наук. Окончила ДГТУ (2000).
Научные интересы: изучение корректирующих способностей помехоустойчивых кодов по отношению к ошибкам различных типов; моделирование источников ошибок цифровых q-ичных каналов связи.
Автор 30 публикаций.

СУХОСТАВСКАЯ Ксения Сергеевна. Окончила ДГТУ (2006), специальность «Компьютерная безопасность».
Научные интересы: изучение характеристик модифицированных помехоустойчивых кодов.